

**METHOD AND APPARATUS FOR PROTECTING AN EXPONENTIATION  
CALCULATION BY MEANS OF THE CHINESE REMAINDER THEOREM (CRT)**

ABSTRACT

5 In a method for protecting an exponentiation calculation by  
means of the Chinese remainder theorem, in particular the  
combining step (16), wherein the Garner combination algorithm  
is preferably used, is verified for its correctness prior to  
10 outputting (24) the results of the combining step (18). In  
doing so, the combination algorithm is verified directly prior  
to outputting the result of the exponentiation calculation, so  
as to eliminate the outputs of an incorrect result, for  
example due to a hardware error attack, so as to ward off the  
15 error attack.

Figure 1